Robustness Analysis of Real Network Topologies Under Multiple Failure Scenarios

Manzano, M. ; Marzo, J. L.; Calle, E.; Fagertun, Anna Manolova

Published in:
2012 17th European Conference on Networks and Optical Communications (NOC)

Link to article, DOI:
10.1109/NOC.2012.6249941

Publication date:
2012

Robustness Analysis of Real Network Topologies Under Multiple Failure Scenarios

M. Manzano*, J. L. Marzo*, E. Calle*, A. Manolova†
*Institute of Informatics and Applications (IIiA)
University of Girona, Spain
{mmanzano, marzo, eusebi}@eia.udg.edu
†Department of Photonics Engineering Networks Technology and Service Platforms
Technical University of Denmark, Denmark
anva@fotonik.dtu.dk

***Abstract*—Nowadays the ubiquity of telecommunication networks, which underpin and fulfill key aspects of modern day living, is taken for granted. Significant large-scale failures have occurred in the last years affecting telecommunication networks. Traditionally, network robustness analysis has been focused on topological characteristics. Recently approaches also consider the services supported by such networks. In this paper we carry out a robustness analysis of five real backbone telecommunication networks under defined multiple failure scenarios, taking into account the consequences of the loss of established connections. Results show which networks are more robust in response to a specific type of failure.**

***Index Terms*—Complex networks, Large-scale failures, Robustness metrics.**

I. Introduction

Failures of great significance (natural or man-made disasters) have occurred on large-scale networks affecting considerable proportions of the world's inhabitants. For example, in 2010 a heavy snowfall in Spain caused a fault in a high tension power cable that left 220 000 people in and around the Catalonian city of Girona without electricity [1]. Further, in February of 2012, four undersea data cables, which were providing connectivity between Europe, the Middle East and East Africa, were cut off by two different shipping accidents and affected millions of Internet and phones users [2].

These large-scale networks consist, mainly, of *nodes* (petrol or underground stations, transformers, etc.), *links* (roads, pipes, cables, etc.) and *dynamic processes* that run over them (oil or gas, trains, electricity, etc.). In this paper we focus on telecommunication networks where nodes represent routers, links the physical (or logical) interconnections between them, and connections the dynamic processes.

With the purpose of studying the impact on the performance of any given service provided by telecommunication networks, lately, researchers have been focused on evaluating the robustness of networks in the case of multiple failure scenarios.

The traditional definition of *robustness*, which relies on graph theory, is mainly centered on graph connectivity. In this paper we assume a more contemporary definition which according to [3] is "the ability of a network to maintain its total throughput under node and link removal". The latter takes into consideration the dynamic processes that run over a network (which in this paper are connections) while the former does not. Further, robustness metrics have been defined in the past years with respect to both approaches.

TABLE I
Classical and contemporary robustness metrics

Approach	Characteristic	Reference
Classical	Average nodal degree (AND)	[4]
	Node connectivity	[5]
	Heterogeneity	[6]
	Symmetry ratio	[7]
	Diameter	[8]
	Average shortest-path length (ASPL)	[9]
	Assortativity coefficient	[4]
	Average neighbor connectivity	[4]
	Clustering coefficient	[10] [4]
	Betweenness centrality	[11]
	Largest eigenvalue	[4] [12]
	Second smallest Laplacian eigenvalue	[13]
	Average two-terminal reliability (A2TR)	[14]
Contemporary	Elasticity	[3]
	Quantitative Robustness Metric (QNRM)	[15]
	R-value	[16]

The aim of this paper is to carry out a robustness analysis, in the case of multiple failures, of five real telecommunication networks when considering both type of metrics: those relying on graph theory aspects and those considering the impact upon connections.

The paper is structured as follows. In Section II several well-known robustness metrics are presented. Section III defines a brief taxonomy of different multiple failure scenarios. The set of real networks is presented in Section IV. Then, the simulation scenario is detailed in Section V and the analysis' results are shown and discussed in Section VI. Finally, in Section VII conclusions and further work are provided.

II. Robustness metrics

This section presents a brief background of several well-known robustness metrics which are considered in the analysis conducted in this paper. As previously mentioned, literature offers a wide range of robustness metrics. Some of them are mainly focused on graph theory concepts while others take into consideration the services supported by networks.

Table I shows a list of robustness metrics separated in two main groups: classical and contemporary. These two groups are not centered on the chronological order of *publication* of the metrics, but on what *robustness definition* rely on. The thirteen classical metrics rely on basic graph theory concepts while the four contemporary ones consider additionally the dynamic services that run over a network. It is important to note that, some of the metrics classified here as *classical* could be considered *contemporary* (the largest eigenvalue or the second smallest laplacian eigenvalue).

In this paper we carry out a robustness analysis from both points of view. While we take into account all metrics from the classical approach, we only consider the *Quantitative Robustness Metric* (*QNRM*) from the contemporary one. The *QNRM* analyses how a multiple failure affects the number of connections established on a network. It provides an accurate value of the *blocked connections* (a connection that should have been established at time t but could not be established as a consequence of a failure).

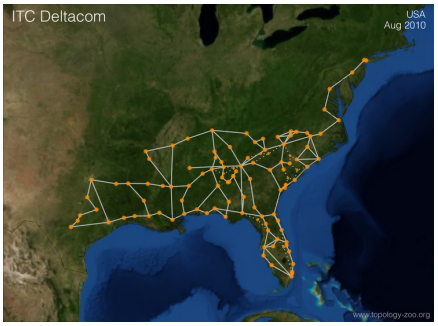
III. Multiple failure scenarios

According to Shang et al [17], when an object that causes an attack knows exact information related to the network topological structure, it is called an attack with white-information (targeted). However, when the attacker knows no information at all, it is considered a black-information attack (random). The former would be more related with intentional failures while the latter would be with component failures or natural disasters. Consequently, multiple failure scenarios proposed in the literature can be broadly classified as either random or targeted scenarios and in this section we present a simple taxonomy of them:

- *Random*: In a random multiple failure, nodal or link failures occur selecting the elements at random. Natural disasters are an example and may have catastrophic consequences on the services supported by a network.
- *Targeted*: Elements in a targeted multiple failure are chosen in order to maximize the impact of it there is an element of discrimination. The choice of the targeted element/s may be a function of network-defined features such as nodal degree or clustering, as well as other "real-world" features, such as the number of users potentially affected and socio-political and economic considerations.

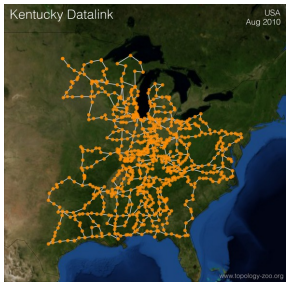
In addition, both types can be either *static* or *dynamic*. Static multiple failures are essentially one-off failures that affect one or more elements (nodes or links) at any given point. Dynamic failures have a temporal dimension. Four main types of multiple failures arise from this taxonomy: *Random Static* (RS), *Random Dynamic* (RD), *Targeted Static* (TS) and *Targeted Dynamic* (TD). In the analysis of this paper we focus on RS and RD.

(a) cogentco

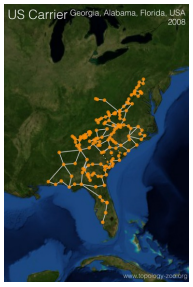


(b) deltacom

(c) ion



(d) kdl



(e) uscarrier

Fig. 1. Networks' layout

IV. Networks

The five real topologies considered in analysis are *cogentco*, *deltacom*, *ion*, *kdl* and *uscarrier*, and layout can be observed in Fig 1. Some of them are backbone transport networks (representing real physical links), others are logical networks (representing the IP layer). They have been obtained from [18], a repository of well known real telecommunication networks.

Table II shows the key characteristics of the topologies described above. Additionally, some characteristics are presented with their *standard deviation*. It can be observed that while some of them have a *number of nodes* that range between 100

and 200, one (*kdl*) has a higher value of it. All networks have a negative or near to zero value of *assortativity coefficient* (r). This means that they have an excess of radial links, links connecting nodes of dissimilar degrees. Such a property is typical on technological networks [19]. The five networks considered in this paper have a similar *average nodal degree*, ranging from 2 to 3.

V. Simulation Scenario

In order to calculate the *Quantitative Robustness Metric* (*QNRM*) the simulation scenario, which is related to the results presented in VI-B, must be detailed. All simulations last for 10 000 time steps with a traffic load of 80 000 connections in total. Source and destination of connection has been selected randomly with the restriction that they cannot be adjacent (connections are minimum of two hops). There is no constraint link capacity, if there are no failures, all connections are accepted. The generation of the connections and their duration follow negative exponential distribution with average inter-arrival and holding times of 0.12 and 100 time steps respectively.

Simulations causing the following multiple failures are carried out:

- RS: A random static multiple failure that affects 10% of nodes of the network is activated at the start of the simulation.
- RD: The *Susceptible-Infected-Disabled* (SID) epidemic model [20] is used in this case study. A dynamic epidemic failure that initially affects 3% of nodes is activated at the start of the simulation, reaching a total of 10% of affected nodes after a period of time (this period is different for each topology and depends upon its specific topological features). The randomness of this case relies on the initial set of infected nodes, which is selected randomly.

The presented results are the average of 200 simulation runs with different random seeds. They show how the set of real network topologies performs in response to either RS or RD, when both affect the same number of nodes. As mentioned in Section II, the *QNRM* metric, which measures the number of blocked connections, is calculated during the simulations.

VI. Results

Two sets of analysis are presented here. First, classical robustness metrics are analyzed and a ranking of the topologies based on the metrics is listed. Second, a robustness analysis in relation to the contemporary robustness metric is presented.

A. Classical robustness analysis

Fig. 2 shows the *Average Two-Terminal Reliability* (*A2TR*) of the five networks. This metric is the probability that a randomly chosen pair of nodes is connected (if the network is fully connected the value of *A2TR* is 1). Therefore, the higher, the better. Because not all of them have the same number of nodes, the number of nodes removed has been uniformed for each one of the networks, in order to plot them all in one graphic. As it can be observed, it would be difficult to rank

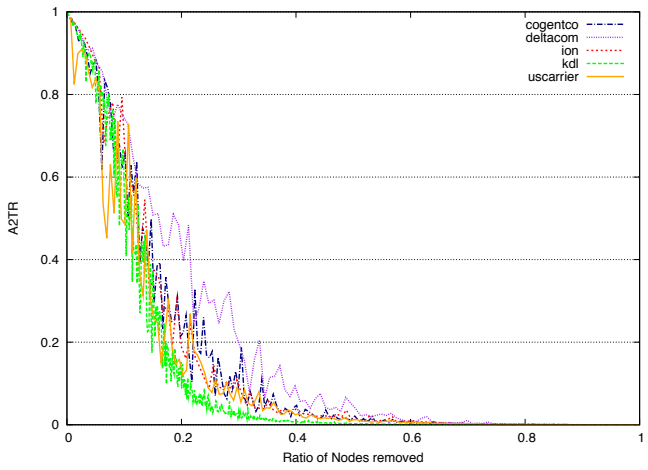


Fig. 2. Average Two-Terminal Reliability of the set of real network topologies

the set of networks according to their *A2TR* evolution, because all of them have a similar *average nodal degree*. However, it is clear that the *deltacom* network is the most robust one. The rest of them have roughly similar curves, although the *kdl* network is the first one that reaches values near 0.

Table III presents a classification based on the features of the topologies of Section IV. In this classification *1* represents the most robust with increasing rank representing reduced robustness. The last row indicates the global ranking of the topologies and is the simple unweighted average of the positions of the previous rankings of each topology. This average could be calculated using different weights for each kind of metric, depending on the specific necessity of the network service provider. However, in the first instance, we consider all the metrics to be equal and will consider the option of a weighted average in future work.

As it can be seen in Table III, on the first row the ranking of *average nodal degree* (*AND*) is provided. This is the coarsest connectivity feature of any topology. Networks with higher *AND* are "better-connected" on average, and, consequently, are likely to be more robust. The most robust network is *deltacom*, followed by *cogencto*, while the less robust one (which has the lowest value of *AND*) is *ion*.

On the second row, the five networks are ranked by their *node connectivity* and all of them have the same value of it (1). Consequently, all of them are ranked equally. It was not expected that real networks could be disconnected by removal of just one node. Regarding the *heterogeneity*, *ion* is the most robust topology, while *deltacom* and *cogentco* are the worst ones. The grading of *average shortest-path length* (*ASPL*) is shown on the following row and as it can be observed, *deltacom* and *ion* are positioned as the most robust topologies. Long-path connections have a higher probability of being affected in the case of multiple failures. Consequently, the lowest the *ASPL* of a network, the robust.

Thereafter, rankings of the *largest eigenvalue* and the *second smallest laplacian eigenvalue* show interesting results. Most

TABLE II
CHARACTERISTICS OF THE SET OF REAL TELECOMMUNICATION NETWORK TOPOLOGIES

Characteristic	cogentco	deltacom	ion	kdl	uscarrier
Number of nodes	197	113	125	754	158
Number of links	242	161	146	895	189
Average nodal degree (AND)	2.46	2.85	2.34	2.37	2.39
Stdev	1.04706	1.21171	0.082251	0.84254	0.8204
Minimum nodal degree	1	1	1	1	1
Node connectivity	1	1	1	1	1
Heterogeneity	0.42563	0.42516	0.03515	0.35550	0.34326
Symmetry ratio	6.79310	4.70833	4.80769	12.77966	4.36111
Diameter	28	23	25	58	35
Average shortest path length	10.52	7.16	10.14	22.73	12.09
Stdev	5.09079	3.79633	4.78563	10.64351	6.45623
Largest eigenvalue	3.77828	3.88918	2.95511	3.16819	2.98417
Second smallest Laplacian eigenvalue	0.00857	0.02235	0.01331	0.00194	0.0056
Clustering coefficient	0.12884	0.14197	0.0992	0.08404	0.10886
Assortativity coefficient	0.01956	0.03832	-0.2797	-0.10462	-0.09518
Average neighbor connectivity	0.0148	0.03	0.02115	0.00354	0.01701
Average node Betweenness centrality	0.04883	0.0555	0.07428	0.02889	0.7109
Stdev	0.06719	0.06983	0.07136	0.03873	0.10082
Average link Betweenness centrality	0.00361	0.00274	0.00638	0.00225	0.0056
Stdev	0.00425	0.00277	0.00516	0.00285	0.00728

TABLE III
RANKING OF ROBUSTNESS OF THE SET OF REAL TELECOMMUNICATION NETWORK TOPOLOGIES, BASED ON TOPOLOGICAL FEATURES

	cogentco	deltacom	ion	kdl	uscarrier
Average nodal degree	2	1	5	4	3
Node connectivity	1	1	1	1	1
Heterogeneity	5	4	1	3	2
Average shortest path length	3	1	2	5	4
Largest eigenvalue	2	1	5	3	4
Second smallest Laplacian Eigenvalue	3	1	2	5	4
Average neighbor connectivity	4	1	2	5	3
Assortativity coefficient	2	1	5	4	3
Symmetry ratio	4	2	3	5	1
Clustering coefficient	2	1	4	5	3
Average node Betweenness centrality	2	3	4	1	5
Average link Betweenness centrality	3	2	5	1	4
Global Ranking	(2.75) 2	(1.58) 1	(3.25) 4	(3.5) 5	(3.08) 3

networks with high values for the *largest eigenvalue* have a small diameter and are more robust. The *second smallest laplacian eigenvalue* measures how difficult it is to break the network into islands or individual components (the larger, the greater the robustness of a topology against both node and link removal). Although both of them rank *deltacom* as the most robust network, there is no match between the 2^{nd} and the 3^{rd} most robust topologies (the *largest eigenvalue* ranks *cogentco* as the second most robust while the *second smallest laplacian eigenvalue* ranks *ion*).

The following two rows show the classification based on the *average neighbor connectivity* and on the *assortativity coefficient*. *deltacom* is the most robust because it has the highest values of them, implying that this network is less vulnerable under any kind of static failures (random or targeted). Regarding the *symmetry ratio* it can be observed that *uscarrier* is the most robust network because it has the lowest value of it. On high-symmetric networks, with low symmetry values, the impact of losing a node does not depend on which node is lost.

Next, the *clustering coefficient* grading shows that *deltacom* is the most robust, its nodes are more interconnected with their neighbors. Finally, from the two rankings of *betweenness centrality* (*BC*) it can be observed that *kdl* is better than *deltacom* because the latter has a higher value of it. This means that *deltacom* has an excess of centrality of some elements that increases the vulnerability of targeted failures.

To summarize the ranking provided in Table III, a global ranking has been calculated and listed in the last row. This final summary ranking gives an approximation to the robustness of the networks considered in this paper, taking into account the traditional robustness metrics, which omit considerations about any connections on the network. Here, *deltacom* is the most robust, followed by *cogentco* in second place. *uscarrier*, *ion* and *kdl* are ranked in third, fourth and fifth place respectively. It is interesting to note that, if the global ranking had not been calculated with the same weights for all the metrics, this ranking would have changed.

Some metrics differ in identifying the 1^{st}, 2^{nd} and 3^{rd} most robust topologies. This means that one should really use a group of metrics to define the robustness rather than rely on single graph robustness metric. Considering several graph

based robustness metrics is necessary, but such an approach would not be sufficient for a network provider, because it does not take into account the connections that run over networks and does not give any information about the service performance of a network under any kind of multiple failure.

B. New robustness metric analysis

The results of the simulations carried out in this paper, which have been detailed previously in Section V, are presented. In Table IV results associated with the *QNRM* metric can be observed. Table IV is divided as follows: rows 1 to 3 pertain to the behavior of the network in response to a RS multiple failure while 4 to 6 pertain to the metric's value in response to an RD. The last two rows show the relation between the RD and the RS in order to facilitate a comparison between the robustness of the networks when either a RS or a RD failure occurs.

Regarding RS multiple failure, the most robust topology is *deltacom*, blocking 35% of the connections that should be established, when a RS multiple failure affects 10% of the nodes. Further, the 2^{nd} most robust topology is *cogentco*, blocking around 36% of the connections, while the 3^{rd} most robust is *kdl*, blocking almost 37% of them. Therefore, the difference between these networks is not significant and the three of them can be considered equally regarding a RS multiple failure. *ion*, which is placed in 4^{th} position, blocks almost 50% of the connections, and *uscarrier* is the less robust one blocking almost 68% of the connections that should be established.

In response to a RD failure the ranking is completely different. Here *uscarrier* is the most robust, blocking around 20% of the connections and *ion* is the 2^{nd} most robust blocking around 27%. It is interesting to note that, *deltacom* is the least robust in response to a RD multiple failure, blocking almost 75% of the connections. This was not expected because *deltacom* has the highest value of *largest eigenvalue* (also known as *epidemic threshold*), which correlates with the severity of an epidemic failure (RD) on a network.

With the purpose of comparing results regarding both types of multiple failures, the last row of Table IV shows a classification of the topologies sorted by the ratio. *uscarrier* is the topology that shows the most improvement in its performance when comparing a RS and a RD multiple failure; the number of blocked connections reduces almost 30% when an epidemic failure (RD) occurs. Second (*ion*) and third (*cogentco*) position networks have a ratio under the unity, which means that they perform better in response to a RD multiple failure than to a RS one. *deltacom* is the topology that shows the least improvement in its performance when comparing both RS and RD.

C. Discussion

Metrics shown in Table III represent a relatively simplistic approach to define the robustness of a network because the metrics do not take into account the connections that are running over the network. Comparing the results shown in Table III with the ones shown in Table IV one may notice that just few positions of the rankings match. For example, in Table III *deltacom* appears to be the most robust network. Moreover, while in Table IV it appears to be the most robust in response to a RS multiple failure it is the least robust in response to a RD. Therefore, classical robustness metrics prove to be useful indicating *general robustness* while contemporary robustness metrics provide more detailed information about it.

VII. Conclusions and future work

In this paper a robustness analysis of five real telecommunication networks has been carried. Well-known robustness metrics have been considered. Further, we have defined a brief taxonomy of multiple failure scenarios and from the types, we have considered *Random Static* (RS) and *Random Dynamic* (RD) in our simulation scenario. The utility of combining classical robustness metrics (relying on graph theory concepts) with those more contemporary, which consider the services carried by networks, has been shown.

Results of have shown that according to the ranking provided by the graph robustness metrics, *deltacom* is the most robust network, *cogentco* is the second most robust and *kdl* (the network with a higher number of nodes) is the least robust. However, if the information provided by this ranking is complemented with the results given by the *QNRM* metric, a network provider is able to know how the services will be affected in response to a given type of multiple failure scenario. For example, *QNRM* shows that *deltacom* is the worst network (least robust) in response to a RD multiple failure affecting 10% of nodes, because it blocks almost 75% of the connections that should be established. Additionally, *QNRM* shows that *uscarrier* is the worst network when RS multiple failure affecting 10% of nodes is caused, because it blocks almost 68% of the connections. Therefore, this information would not be known if only graph robustness metrics were taken into account. It demonstrates that both approaches (classical and contemporary) should be considered by network providers. Moreover, regarding to the set of real telecommunication networks considered in this work, it can be observed that some networks have been (casually or not) designed to be more robust in response to a specific kind of failure (for example, *deltacom* or *uscarrier*).

There are some aspects that could be considered as future work. For instance, assuming that all the results provided in this paper have been obtained considering an infinite capacity of links and a unique traffic pattern, it could be interesting to carry out the analysis within a simulation scenario of finite capacity. Comparing both results (the ones obtained from infinite capacity simulations and the ones from finite capacity) it could be possible to know how many connections would be lost due to capacity. Moreover, it could be interesting to carry out analysis (with both finite and infinite capacity) using different traffic patterns, in order to know what network is more suitable (in terms of robustness) for a specific traffic pattern.

TABLE IV
QUANTITATIVE ROBUSTNESS METRIC RESULTS OF THE SET OF REAL TELECOMMUNICATION NETWORK TOPOLOGIES

Impairment		cogentco	deltacom	ion	kdl	uscarrier
Random Static (RS)	QNRM	0.3634	0.3477	0.4881	0.3678	0.6797
	Standard Deviation	0.00052	0.0005	0.0005	0.00053	0.00072
	Ranking	2	1	4	3	5
Random Dynamic (RD)	QNRM	0.2826	0.7478	0.2624	0.4257	0.2039
	Standard Deviation	0.00196	0.010833	0.04608	0.00738	0.01498
	Ranking	3	5	2	4	1
	$\frac{QNRM_{RD}}{QNRM_{RS}}$	0.7776	2.1507	0.5375	1.1574	0.2999
	Ratio Ranking	3	5	2	4	1

ACKNOWLEDGMENT

This work is partly supported by the Spanish Ministerio de Ciencia e Innovacion through project TEC 2009-10724 and by the Generalitat de Catalunya through the research support program project SGR-1202 and AGAUR FI-DGR 2012 grant.

REFERENCES

[1] J. Sturcke, "Spanish snow leaves 250 000 without power," *The Guardian*, March 2010.

[2] S. Moore, "Ships sever data cutting east africa links," *The Wall Street Journal*, p. B3, February 2012.

[3] A. Sydney, C. M. Scoglio, P. Schumm, and R. E. Kooij, "Elasticity: Topological characterization of robustness in complex networks," in *Proceedings of the 3rd International Conference on Bio-Inspired Models of Network, Information and Computing Sytems*, Brussels, Belgium, 2008, pp. 19:1–19:8.

[4] P. Mahadevan, D. Krioukov, M. Fomenkov, X. Dimitropoulos, K. C. Claffy, and A. Vahdat, "The internet as-level topology: three data sources and one definitive metric," *SIGCOMM Computer Communications Rev.*, vol. 36, pp. 17–26, January 2006.

[5] A. H. Dekker and B. D. Colbert, "Network robustness and graph topology," in *Proceedings of the 27th Australasian conference on Computer science - Volume 26*. Darlinghurst, Australia: Australian Computer Society, Inc., 2004, pp. 359–368.

[6] J. Dong and S. Horvath, "Understanding Network Concepts in Modules," *BMC Systems Biology*, vol. 1, no. 1, 2007.

[7] A. H. Dekker and B. Colbert, "The symmetry ratio of a network," in *Proceedings of the 2005 Australasian symposium on Theory of computing - Volume 41*, ser. CATS '05. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2005, pp. 13–20.

[8] E. W. Weisstein, "Graph diameter," http://mathworld.wolfram.com/GraphDiameter.html, from MathWorld–A Wolfram Web Resource.

[9] C. Shannon and D. Moore, "The spread of the witty worm," *IEEE Security and Privacy*, vol. 2, pp. 46–50, 2004.

[10] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, Jun. 1998.

[11] L. C. Freeman, "A set of measures of centrality based upon betweenness," *Sociometry*, vol. 40, no. 1, pp. 35–41, 1977.

[12] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos, "Epidemic thresholds in real networks," *ACM Transactions on Information and System Security*, vol. 10, no. 4, pp. 1–26, 2008.

[13] A. Jamakovic and S. Uhlig, "Influence of the network structure on robustness," in *Proceedings of the 15th IEEE International Conference on Networks, ICON 2007, 19-21 November 2007, Adelaide, Australia*, 2007, pp. 278–283.

[14] S. Neumayer and E. Modiano, "Network reliability with geographically correlated failures," in *Proceedings of the 29th conference on Information communications*, ser. INFOCOM'10. Piscataway, NJ, USA: IEEE Press, 2010, pp. 1658–1666.

[15] M. Manzano, E. Calle, and D. Harle, "Quantitative and qualitative network robustness analysis under different multiple failure scenarios," in *Proceedings of the 3rd International Workshop on Reliable Networks Design and Modeling (RNDM)*, oct. 2011, pp. 1–7.

[16] P. V. Mieghem, C. Doerr, H. Wang, J. M. Hernandez, D. Hutchison, M. Karaliopoulos, and R. E. Kooij, "A framework for computing topological network robustness," 2010, Delft University of Technology, Report20101218. [Online]. Available: http://www.nas.ewi.tudelft.nl/people/Piet/TUDelftReports

[17] Y. Shang, "Robustness of scale-free networks under attack with tunable grey information," *EPL (Europhysics Letters)*, vol. 95, no. 2, p. 28005, 2011.

[18] http://www.topology-zoo.org/, [Online; accessed 11-April-2012].

[19] M. E. J. Newman, "The structure and function of complex networks," *SIAM Review*, vol. 45, pp. 167–256, 2003.

[20] E. Calle, J. Ripoll, J. Segovia, P. Vilà, and M. Manzano, "A multiple failure propagation model in GMPLS-based networks," *IEEE Network*, vol. 24, pp. 17–22, November 2010.